## REMARKS

By this amendment, claims 1-29 are pending, in which claims 1 and 28 are currently amended. No new matter is introduced. These changes are not believed to raise new issues requiring further consideration and/or search, and it is therefore respectfully requested that the present amendment be entered under 37 C.F.R. §1.116.

The final Office Action mailed January 27, 2005 rejected claims 1-27 as obvious under 35 U.S.C. § 103 based on *Bector et al.* (US 6,687,732) in view of *McCanne et al.* (US 6,611,872); and rejected claims 28 and 29 under 35 U.S.C. § 103 based on *Bector et al.*

Applicant respectfully disagrees with the arguments asserted in the Final Office Action, pages 2 and 3. Specifically, the claims do indeed clearly define the functions of the tracking router. For example, independent claim 14 recites an "ingress edge router rerouting the DoS flood attack datagram to the **tracking router as to permit identification of the ingress edge router**." This recitation corresponds to operation of the tracking router, as explained, for instance, on page 10, lines 16-18 of the Specification:

> In the system of Figure 1, tracking router 125 forms an overlay network with edge routers 109, 111, 113, and 115 to track down the ingress edge router that is responsible for forwarding the packet flood attacks into ISP network 101.

The Final Office Action correctly acknowledges that *McCanne* fails to disclose "ingress edge router rerouting the DoS flood attack datagram to the **tracking router as to permit identification of the ingress edge router**." However, the Examiner never states that this absent feature can be found in *Bector*, as the Examiner merely concludes "Bector discloses that is its [sic] known for routers to perform security diagnostics, which include identifying a DOS attack, and rerouting the malicious datagram to an overlay network. It would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the security functions

as taught by Bector, since Bector states at column 4, lines 2-54 that such a modification would increase network security." The lengthy cited passage of col. 4: 2-54, states the following (*Emphasis Added*):

> A system, method and mechanism are provided that address the problems enumerated above. In particular, **a system, mechanism and method are provided for dynamically determining whether to dispatch traffic to a local proxy server, or to bypass the proxy server to send the traffic to a remote server or to the original target origin server.** Various embodiments are provided that can:
>
> recognize packets that carry malformed or out-of-spec protocol traffic, and bypass them to the origin server without transfer to the proxy processing engine;
>
> recognize packets that are presented in a foreign or unprocessable protocol, and bypass them to the origin server without transferring them to the proxy processing engine;
>
> recognize network traffic that cause semantic changes or errors related to IP identification and proxy-based IP address changes, and bypass this traffic directly to the origin server, preserving the client IP address;
>
> detect overloaded redirection targets, and bypass quantities of traffic directly toward origin servers, and away from interception target applications, to prevent overload;
>
> detect known problematic clients or servers, bypass traffic directly toward origin servers, and away from interception target applications;
>
> efficiently maintain distributed lists of clients and servers that wish not to be processed by intercepting applications, bypass this traffic directly toward origin servers, and away from interception target applications; and
>
> identify classes of transactions that will not gain value from redirection to intercepting servers, and efficiently bypass this traffic directly toward origin servers, and away from interception target applications.
>
> **Further, because intercepting proxies are central intermediaries, and because redirection target applications can fail, a system, method and mechanism are provided that can detect non-functional redirection targets, and bypass traffic directly toward origin servers, and away from interception target applications.**
>
> Similarly, because intercepting proxies are central intermediaries, and because malicious clients may be able to construct schemes to interfere with the correct

> operation of these intermediaries, denying service to all users, **a system, method and mechanism are provided that can detect malicious attacks, and bypass traffic directly toward origin servers, and away from interception target applications, to minimize the risk of denial of service attacks.**
>
> The foregoing needs, and other needs that will become apparent from the following description, are addressed by the systems, methods and methods that are described in this disclosure.

As evident from the above passage, at best, there is a general discussion of a mechanism to detect malicious attacks, bearing no relevance to "ingress edge router rerouting the DoS flood attack datagram to the **tracking router as to permit identification of the ingress edge router**." 35 U.S.C. § 132 requires the Director to "notify the applicant thereof, stating the reasons for such rejection." This section is violated if the rejection "is so uninformative that it prevents the applicant from recognizing and seeking to counter the grounds for rejection." *Chester v. Miller*, 15 USPQ2d 1333 (Fed. Cir. 1990). This policy is captured in the Manual of Patent Examining Procedure. For example, MPEP § 706 states that "[t]he goal of examination is to clearly articulate any rejection early in the prosecution process so that applicant has the opportunity to provide evidence of patentability and otherwise respond completely at the earliest opportunity." Furthermore, MPEP § 706.02(j) indicates that: "[i]t is important for an examiner to properly communicate the basis for a rejection so that the issues can be identified early and the applicant can be given fair opportunity to respond." Unfortunately, the Examiner's only discussion of this limitation is a vague reference to a seemingly irrelevant passage.

Regarding the Examiner's reference to *ipsissimis verbis* (Office Action, page 2, item 6), Applicant understands that the identity of terminology is not required, but instead contends that the elements that are taught by *Bector* and *McCanne* are not read on by the claims. In this instance, the terms are not identical because the claims are distinguishable from the applied art. Additionally, Applicant acknowledges that the Examiner is entitled to the broadest reasonable

interpretation of the claims; this principle, however, does not entitle the Examiner to simply ignore claim terms, notably "tracking." That is, it is improper to ignore qualifiers in the claim terms such as "tracking router" See *Apple Computer, Inc. v. Articulate Systems, Inc.*, 234 F.3d 14 (Fed. Cir. 2000) (holding that the district court "cannot read the qualifier 'help' out the definition of 'help access window'" of claim 2).

In the interest of advancing prosecution, Applicants amended independent claims 1 and 28 recite "**identifying, by the tracking router, an ingress edge router** that forwarded the DoS flood attack datagram." As explained with respect to claim 14, the even the combination of *Bector et al.* and *McCanne* does not satisfy this feature.

In view of the above arguments, Applicant respectfully requests withdrawal of the obviousness rejections, and urges the indication that independent claims 1, 14, and 28, along with their corresponding dependent claims 2-13, 15-27, and 29, be allowable.

Therefore, the present application, as amended, overcomes the objections and rejections of record and is in condition for allowance. Favorable consideration is respectfully requested. If any unresolved issues remain, it is respectfully requested that the Examiner telephone the undersigned attorney at (703) 425-8508 so that such issues may be resolved as expeditiously as possible.

Respectfully Submitted,

DITTHAVONG & CARLSON, P.C.

3/28/05
Date

Phouphanomketh Ditthavong
Attorney/Agent for Applicant(s)
Reg. No. 44658

10507 Braddock Road
Suite A
Fairfax, VA 22032
Tel. (703) 425-8508
Fax. (703) 425-8518